IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TENNESSEE

UNITED STATES OF AMERICA	)	
	)	
v.	)	NO.: 3:08-cr-142
	)	JUDGES PHILLIPS/SHIRLEY
	)	
DAVID C. KERNELL	)	

MEMORANDUM IN SUPPORT OF MOTION TO DISMISS

Comes the Defendant, DAVID C. KERNELL, by and through counsel, pursuant to Rules 7(c) and 12 of the Federal Rules of Criminal Procedure; the Due Process, Grand Jury, and Double Jeopardy Clauses of the Fifth Amendment; the Notice Clause of the Sixth Amendment; Blockburger v. United States, 284 U.S. 299 (1932); Papachristou v. City of Jacksonville, 405 U.S. 156 (1972); Hamling v. United States, 418 U.S. 87 (1974); Apprendi v. New Jersey, 530 U.S. 466 (2000), and their progeny, and hereby moves the Court for an order dismissing the Indictment. The Government has charged Mr. Kernell with violating what should be a misdemeanor provision of the United States Code but, in the same count, the Government has attempted to enhance the charge to a felony by claiming the violation was committed in furtherance of another misdemeanor which functionally prohibits the same conduct.

Primary issues presented: The first issue in this case is whether the Government has improperly joined two misdemeanor provisions in an attempt to create a felony. The second issue is whether the Indictment must be dismissed because this prosecution is based on unconstitutionally vague statutes, potentially applicable without limitation but prosecuted as the exception.

I. INTRODUCTION

The Indictment in this case charges, as a violation of 18 U.S.C. Section 1030, that:

> On or about September 16, 2008, in the Eastern District of Tennessee and elsewhere, defendant DAVID C. KERNELL, in furtherance of the commission of a criminal act in violation of the laws of the United States, including 18 U.S.C. Section 2701 and 18 U.S.C. Section 1030(a)(2), intentionally and without authorization accessed a protected computer by means of an interstate communication and thereby obtained information, and did aid and abet in same.

By these terms, the Government has alleged and must prove that:

> On or about September 16, 2008, in the Eastern District of Tennessee and elsewhere, defendant DAVID C. KERNELL, in furtherance of
>
> > intentionally **accessing** without authorization a facility through which an electronic communication service is provided and thereby obtaining, altering, or preventing authorized access to a wire or electronic communication while it was in electronic storage in such system, [Section 2701] and
> >
> > intentionally **accessing** a computer without authorization and thereby obtaining information from a protected computer when the conduct involved an interstate communication [Section 1030],
>
> intentionally and without authorization **accessed** a protected computer by means of an interstate communication and thereby obtained information, and did aid and abet in same.

Indictment at Count 1; 18 U.S.C. § 2701(a); 18 U.S.C. § 1030(a)(2). In other words, the indictment alleges that David Kernell accessed a computer and obtained information in furtherance of the same conduct charged as the underlying offense.

II. THE INDICTMENT FAILS TO STATE AN OFFENSE BECAUSE IT IS IMPROPER TO AGGREGATE THESE FUNCTIONALLY IDENTICAL MISDEMEANORS INTO A FELONY.

The Indictment charges a greater punishment than Congress intended and thereby fails to state an offense. A violation of section 1030(a)(2) is generally a misdemeanor. 18 U.S.C. § 1030(c)(2)(A). However, when section 1030(a)(2) is violated "in furtherance of" another crime, it becomes a felony punishable by up to five years imprisonment. 18 U.S.C. § 1030(c)(2)(B)(ii).

Here, the Indictment charges a violation of section 1030(a)(2), then seeks a felony enhancement by both re-alleging a violation of section 1030(a)(2) and alleging a violation of section 2701, a statute which prohibits the same conduct as section 1030(a)(2). Stated differently, Mr. Kernell is charged with unauthorized access, a misdemeanor; but because Mr. Kernell is also charged with committing that misdemeanor in furtherance of the same instance of unauthorized access, he is charged with a felony. If the enhancement is allowed to stand and Mr. Kernell is convicted, Mr. Kernell will be punished in excess of the punishment proscribed for his conduct.

To diagram an allegation of unauthorized access in furtherance of the same alleged act of unauthorized access produces a figure much like the mythical Ouroboros swallowing its own tail, because both section 1030 and section 2701 become felonies when violated "in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or any State." 18 U.S.C. § 1030(c)(2)(B)(ii); 18 U.S.C. § 2701(b)(1). Under the government's theory, section 1030 could be used to enhance itself, section 2701 could be used to enhance itself, and each could be used to enhance the other without end.

Fortunately, the Department of Justice's own manual on prosecuting computer crimes confirms that the criminal or tortious act used to enhance a penalty must be a *separate* act: "Naturally, the 'in furtherance of any criminal or tortious act' language means an act *other than* the unlawful access to stored communications itself." Computer Crime & Intellectual Property Section, U.S. Dep't of Justice, *Prosecuting Computer Crimes* 82 (Feb. 2007) available at http://www.usdoj.gov/criminal/cybercrime/ccmanual/index.html (last visited Oct. 21, 2008) [hereinafter Dep't of Justice, *Computer Crime*] (citing Boddie v. American Broadcasting Co., 731 F.2d 333, 339 (6th Cir. 1984)) (emphasis added).

In addition, the Department notes in its manual that the "in furtherance of" language is taken from the Wiretap Act, see 18 U.S.C. § 2511(2)(d), and that at least one appellate court has

stated that this enhancement is operative only when a prohibited purpose is the subject's *primary* motivation or a determinative factor in the subject's motivation. Id. at 82 (citing United States v. Cassiere, 4 F.3d 1006, 1021 (1st Cir. 1993)). An offender's motivation is not the end of the inquiry: *when* the offender formed the requisite motivation is central to whether the "in furtherance of" enhancement applies. The motivation must have been formed in anticipation of committing the additional crime, and sustained long enough to have caused harm. For example, in By-Prod Corp. v. Armen-Berry Co., 668 F.2d 956 (7th Cir. 1982), the Government alleged that the defendant intercepted a telephone call in order to "commit an act that is criminal or tortious under federal or state law." Id. The Seventh Circuit held that even if the Defendant formed the requisite intent to use the intercepted tape recording, his failure to actually use the recording was what mattered, because his wrongful intention was not sustained.

> We doubt [] that a tape recording which was never used could form the basis for liability . . . . It would be a dryly literal reading of the statute that found a violation because at the moment of pressing the "on" button a party to a conversation conceived an evil purpose though two seconds later he pressed the "off" button and promptly erased the two seconds of tape without even playing it back. **A statute that provides for minimum damages of $1000 per violation must have more substantial objects in view than punishing evil purposes so divorced from any possibility of actual harm**.

Id. at 959-60 (emphasis added). See also Stockler v. Garrett, 893 F.2d 856 (6th Cir. 1990) (holding that "interception" and not "use" is all that is required to violate Wiretap Act, but failing to abrogate Boddie's holding that the criminal or tortious purpose must be "other than" the interception and/or use).

If the Government is alleging that unauthorized access was Mr. Kernell's primary motivation, it is logically inconsistent to use the "in furtherance of" aggravating factor when the underlying violation is the same instance of alleged unauthorized access. The act done in furtherance of the underlying act must be "other than" that underlying act. Multiple offenses

should not be combined into a single count and allowed to transform one another into something more than Congress intended. The felony enhancement must be dismissed.

III. THE INDICTMENT IS DUCPLICITOUS BY CHARGING MORE THAN ONE CRIME IN A SINGLE COUNT; BUT HERE THE HARM IS WORSE BECAUSE THE GOVERNMENT SEEKS TO MAKE ONE FELONY FROM TWO MISDEMANORS.

The felony should be dismissed from the Indictment because the Government has attempted to create a felony out of misdemeanors. Both section 1030(a)(2) and section 2701 prohibit unauthorized access to computers, and both are misdemeanors unless committed "in furtherance of any criminal or tortious act." See 18 U.S.C. § 1030(c)(2); 18 U.S.C. § 2701(b). In order to inflate the statutory penalty, the Indictment essentially says that Mr. Kernell accessed a computer without authorization in furtherance of accessing a computer without authorization; moreover, at least in part, the Indictment says that David Kernell violated section 1030(a)(2) for the purpose of violating 1030(a)(2). There is no statutory element or any conduct that would distinguish Mr. Kernell's alleged conduct from conduct constituting a misdemeanor under section 1030. As a matter of logic, congressional intent, and the plain language of the statutes involved, such an attempt to enhance a misdemeanor to a felony must fail. See Dep't of Justice, *Computer Crime* at 82 (providing that "in furtherance of any criminal or tortious act" means an act *other than* the predicate act).

The indictment is duplicitous. More troubling, though, is that the nature of the misdemeanor-to-felony duplicity is such that the punishment is not doubled, it is increased exponentially. A felony conviction does not double the penalty of a misdemeanor: in addition to the significantly greater imprisonment term, the collateral consequences of having been branded a felon last a lifetime.

Double jeopardy analysis instructs whether an indictment charges multiple offenses in a single count. In addition to protecting against subsequent prosecutions for the same offense, the Double Jeopardy Clause protects against multiple punishments for the same offense. North Carolina v. Pearce, 395 U.S. 711, 717 (1969); U.S. Const. amend. V. By extension, the Double Jeopardy Clause protects against duplicitous and enhanced punishments for the same offense. Here, double jeopardy analysis also shows that the two misdemeanor provisions are functionally the same and that multiple punishment is not authorized. "The ban against duplicitous indictments derives from four concerns: (1) prejudicial evidentiary rulings at trial; (2) the lack of adequate notice of the nature of the charges against the defendant; (3) prejudice in obtaining appellate review and prevention of double jeopardy; and (4) risk of a jury's non-unanimous verdict." United States v. Cooper, 966 F.2d 936, 939 n.3 (5th Cir. 1992) (citations omitted). Duplicitous indictments may prevent jurors from acquitting on a particular charge by allowing them to convict on another charge that is improperly lumped together with another offense in a single count. See United States v. Morse, 785 F.2d 771, 774 (9th Cir. 1986).

The mere fact that two convictions are authorized by different statutory provisions does not establish clear legislative intent that Congress specifically authorized cumulative punishment for the same conduct. See Rutledge v. United States, 517 U.S. 292 (1996); Williams v. Singletary, 78 F.3d 1510 (11th Cir. 1996) (no clear indication of legislative intent to authorize cumulative conviction and sentences because no clear language in statute and no indication from state courts or legislature as to how to interpret state law). When, as here, legislative intent is ambiguous, a court must construe the legislative intent according to the test set out in Blockburger v. United States, 284 U.S. 299 (1932), and it must do so with the understanding that "[t]he assumption underlying the rule is that Congress *ordinarily* does not intend to punish the same offense under two different statutes." Missouri v. Hunter, 459 U.S. 359, 366 (1983)

(quoting Whalen v. United States, 445 U.S. 684, 691-92 (1980)). The Blockburger test provides that, "where the same act or transaction constitutes a violation of two distinct statutory provisions, the test to be applied to determine whether there are two offenses or only one, is whether each provision requires proof of a fact which the other does not." Blockburger, 284 U.S. at 304; United States v. Vartanian, 245 F.2d 609, 616 (6th Cir. 2001) (information not duplicitous because charges require proof of distinct facts).

According to the Blockburger test, and as demonstrated by the following chart, this Indictment is duplicitous. Sections 1030(a)(2) and 2701 prohibit the same conduct.

§ 1030(a)(2)	***§ 2701***
Whoever	Whoever
intentionally	intentionally
accesses[1]	accesses
a computer	a facility through which an electronic communication service is provided[2]
without	without
authorization	authorization
and	and
thereby	thereby
obtains	obtains, alters, or prevents unauthorized access to
information	a wire or electronic communication
from any protected computer	while it is in electronic storage in such a system[3]
if the conduct involved an interstate or foreign communication	
shall be punished.	shall be punished.

18 U.S.C. § 1030(a)(2); 18 U.S.C. § 2701(a).

The Department of Justice recognizes that the offenses are generally the same. See Dep't of Justice, *Computer Crime* at 83-84 ("Since its enactment in 1986, there have been very few

[1] Significantly, Congress did not define "access." See Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 889 (9th Cir. 2002) (noting the absence of a statutory definition of "access"); see also *A Thinly Veiled Request for Congressional Action on E-mail Privacy:* United States v. Councilman, 19 Harv. J.L. & Tech 211, 215 (2005) (same); Julie J. McMurry, Note, *Privacy in the Information Age: The Need for Clarity in the ECPA*, 78 Wash. U. L.Q. 597, 619 (2000) (supporting the creating of a statutory definition of access).

[2] "Facilities" are computers. "A provider of email accounts over the internet is a provider of ECS, see FTC v. Netscape Communications Corp., 196 F.R.D. 559, 560 (N.D. Cal. 2000) . . . . Thus, computers which provide such services are facilities through which an ECS is provided. See Snow v. DirectTV, 450 F.3d 1314 (11th Cir. 2006)." DOJ, *Computer Crimes* at 80.

[3] "Electronic communications system" is "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." 18 U.S.C. § 2510(14).

prosecutions under section 2701. . . . [One reason for this lack is that] many violations of section 2701 also involve conduct that violates 18 U.S.C. § 1030."). See also Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1239 (2004) [hereinafter Kerr, *User's Guide*] ("Section 2701 should be repealed because its costs greatly outweigh its benefits. The benefits of § 2701 are quite limited because the statute is almost entirely redundant. Section 1030(a)(2) already covers most of the same ground. . . . [Section] 2701 is at most only a jurisdictional hook that applies in an extremely narrow circumstance. Specifically, § 2701 provides federal jurisdiction for acts of hacking into and otherwise damaging providers of ECS in the rare circumstance that the conduct does not involve an interstate or foreign communication.").

Duplicitous indictments must be dismissed because of the potential to prevent appropriate sentencing. See e.g., United States v. Sturdivant, 244 F.3d 71, 77 (2d Cir. 2001) (count of indictment duplicitous and defendant harmed when judge sentenced as though general jury verdict convicted defendant of both crimes). In Missouri v. Hunter, 459 U.S. 359 (1983), the U.S. Supreme Court altered its stance on multiplicity to hold that "[w]ith respect to cumulative sentences imposed in a single trial, the Double Jeopardy Clause does no more than prevent the sentencing court from prescribing greater punishment than the legislature intended." Id. at 366 (reasoning that legislatures, not courts, prescribe the scope of punishments). See also United States v. Salameh, 261 F.3d 271, 278 (2d Cir. 2001) (count of indictment resulting in two convictions for use of explosive device under same statute not duplicitous because Congress clearly expressed intent to enhance punishment). No such intent has been expressed here.

"The intent of this subsection [1030(a)(2)] is to protect against the interstate or foreign theft of information by computer, not to give federal jurisdiction over all circumstances in which someone unlawfully obtains information via a computer." Dep't of Justice, *Computer Crime* at

17 (citing S. Rep. No. 104-357). Similarly, the intent of the felony enhancement in 1030(c)(2)(B)(ii) is to protect against costly damages and widespread harm, not to transform all misdemeanors for unauthorized access into felonies. See Patricia L. Bellia, *Chasing Bits Across Borders*, 2001 U. Chi. Legal F. 35, 36 (2001) (noting that the "I Love You" computer virus of May 2000 caused a loss estimated at up to $10 billion). Cf. United States v. Cotton, 535 U.S. 625, 634 (2002) ("In providing for graduated penalties in 21 U.S.C. § 841(b), Congress intended that defendants . . . involved in large-scale drug operations receive more severe punishment than those committing drug offenses involving lesser quantities.")

IV. THE INDICTMENT FAILS TO STATE AN OFFENSE BECAUSE IT DOES NOT CONTAIN THE ESSENTIAL ELEMENTS AND FACTS REQUIRED UNDER THE STATUTES.

The Indictment is insufficient because it does not include the elements of the enhancing crime, it omits essential elements of the offense, and it fails to allege all facts necessary to support a violation of § 2701. There are several requirements for an indictment to be considered sufficient. First, there is the "fair notice requirement that the indictment must furnish the defendant with" "such a description of the charge" against him so that he is able to "make his defense." United States v. Cruikshank, 92 U.S. 542, 558 (1875). The Notice Clause of the Sixth Amendment requires that a criminal defendant has the right "to be informed of the nature and cause of the accusation" against him. U.S. Const. amend. VI.; United States v. Maney, 226 F.3d 660, 663 (6th Cir.2000). Second, the indictment must allege the conduct being charged with sufficient particularity that the defendant can raise her conviction or acquittal as a bar to future proceedings based on the same conduct. Hamling, 418 U.S. at 117. That is, the indictment must be sufficiently detailed to "inform the court of the facts alleged, so that it may decide whether they are sufficient in law to support a conviction, if one should be had. Next, the Indictment

Clause of the Fifth Amendment requires that a defendant be charged with only those charges brought before the grand jury. U.S. Const. amend. V.; Maney, 226 F.3d at 663.

> A grand jury, in order to make that ultimate determination, must necessarily determine what the question under inquiry was. To allow the prosecutor, or the court, to make a subsequent guess as to what was in the minds of the grand jury at the time they returned the indictment would deprive the defendant of a basic protection which the guaranty of the intervention of a grand jury was designed to secure. For a defendant could then be convicted on the basis of facts not found by, and perhaps not even presented to, the grand jury which indicted him.

Russell v. United States, 369 U.S. 749, 769-70 (1962).

Consequently, an indictment is not sufficient unless it states all material elements of the offense. Hamling v. United States, 418 U.S. 87, 117 (1974); United States v. Locklear, 97 F.3d 196, 198-99 (7th Cir. 1996). Rule 7(c)(1) of the Federal Rules of Criminal Procedure states, in pertinent part, that "[t]he indictment or the information shall be a plain, concise and definite written statement of the essential facts constituting the offense charged." This rule merely expresses and codifies what the law has always been: it remains essential that every element of an offense be stated so that defendant is given fair notice of the charge against him.[4] See United States v. Hernandez, 980 F.2d 868, 871 (2d Cir. 1992); Honea v. United States, 344 F.2d 798, 803 (5th Cir. 1965).

> The "inclusion of the elements of the offense . . . known as the **"essential elements" requirement**, is based primarily upon a third pleading function, sometimes characterized as the "judicial review" function. That function has been described by the Supreme Court as "inform[ing] the [trial] court of the facts alleged, so that it may decide whether they are sufficient in law to support a conviction, if one should be had." Although this "judicial review" function is mentioned far less frequently than the "notice" and "double jeopardy" functions, it remains a cornerstone of both federal and state pleading requirements.

[4] Mr. Kernell has filed a motion for bill of particulars; however, a bill of particulars will not cure an insufficient indictment. United States v. Salisbury, 983 F.2d 1369, 1375 (6th Cir. 1993); see also Russell v. United States, 369 U.S. 749, 769-770 (1962); United States v. Sturman, 951 F.2d 1466, 1479 (6th Cir.1992).

United States v. Landham, 251 F.3d 1072, 1080, n.4 (6th Cir. 2001) (internal citations omitted) (emphasis added).

Although an indictment that tracks the statutory language defining an offense is usually sufficient, e.g., United States v. Caldwell, 176 F.3d 898, 901 (6th Cir. 1999) (indictment sufficient because tracked statutory language and expressly set forth all elements necessary to constitute offense charged), mere recitation of statutory language is acceptable *only if* all elements of the charged crime are subsumed in the language. See e.g., United States v. Pickett, 353 F.3d 62, 67 (D.C. Cir. 2004).

> Pickett is correct and the Government incorrect. The Government's argument is built on a foundation of selective quotation. True, the indictment tracks the language of the statute. However, the indictment tracks the language of only a portion of the statute. As Rule 7(c)(1) succinctly requires, the indictment "must be a plain, concise, and definite written statement of the *essential facts constituting the offense charged*." . . . As the Supreme Court taught in *Russell*, it is a fundamental "protection[ ] which an indictment is intended to guarantee," that the indictment "contain[ ] the elements of the offense intended to be charged and sufficiently apprise the defendant of what he must be prepared to meet." While the Government is correct that indictments have been upheld where they tracked the language of the statute, *see, e.g., United States v. Lang, supra*, this indictment tracks only part of the statutory language. . . .

United States v. Pickett, 353 F.3d 62, 67 (D.C. Cir. 2004) (internal citations omitted).

The omission of an essential element of the offense from the indictment cannot be cured by a citation to the applicable statute. See id. at 549 (citing United States v. Hooker, 841 F.2d 1225, 1227-28 (4th Cir. 1988) (reversing RICO conspiracy conviction on basis that indictment did not allege all essential elements of the offense even though jury instructions did)).

> "It is elementary that every ingredient of crime must be charged in the bill, a general reference to the provisions of the statute being insufficient." We have repeatedly reaffirmed this rule in subsequent cases.

United States v. Hooker, 841 F.2d 1225, 1227-28 (4th Cir. 1988) (internal citations omitted). By these standards, and for the following reasons, the indictment is insufficient.

a. *The indictment violates the Sixth Amendment because it does not contain the elements of the offense that the Government purports to use to enhance the offense to a felony.*

The Indictment does not include the elements of section 2701, the enhancing crime, in violation of Apprendi v. New Jersey, 530 U.S. 466 (2000). In Apprendi, the U.S. Supreme Court held that "[o]ther than the fact of a prior conviction, any fact that increases the penalty for a crime beyond the prescribed statutory maximum must be submitted to a jury, and proved beyond a reasonable doubt," id. at 490, because

> [i]f a defendant faces punishment beyond that provided by statute when an offense is committed under certain circumstances but not others, it is obvious that both the loss of liberty and the stigma attaching to the offense are heightened; it necessarily follows that the defendant should not-at the moment the State is put to proof of those circumstances-be deprived of protections that have, until that point, unquestionably attached.

Id. at 484. Prior to Apprendi, the Court had held that an indictment "need not set forth factors relevant only to the sentencing of an offender found guilty of the charged crime." Almendarez-Torres v. United States, 523 U.S. 224, 228 (1998). However, two years after Apprendi, the Court had the opportunity to confirm that the Sixth Amendment requires that "any fact that increases the penalty for a crime beyond the prescribed statutory maximum" must be charged in the indictment. United States v. Cotton, 535 U.S. 625, 627 (2002) (finding indictment unconstitutional which failed to allege a fact, drug quantity, that increased the statutory maximum sentence).

An enhancement must be charged in the indictment because "a criminal indictment holds a central place under the U.S. Constitution." United States v. Thompson, 515 F.3d 556, 566 (6th Cir. 2008) (insufficient indictment). See also United States v. Payne, 173 Fed.Appx. 429, 432 (6th Cir. 2006) (vacating application of sentencing enhancement where firearm type not charged in indictment). Because there are multiple ways in which section 2701 may be violated, Mr.

Kernell must be given sufficient notice of the charge against him. The elements of section 2701 are not merely relevant to sentencing; because the government has alleged an enhancing crime to convert the misdemeanor 1030(a)(2) into a felony, section 2701 increases the penalty beyond the statutory maximum and the Constitution mandates that that this should have been brought before a Grand Jury and charged in the indictment.

b. *The Indictment is insufficient because the Government has not alleged any facts which would establish a violation of § 2701.*

There are insufficient facts in the Indictment to support a violation of § 2701. Specifically, there is no allegation that David Kernell read unopened emails as required before liability is imposed. Indictment ¶¶ 1-10.

As more fully discussed in the Section V, *infra*, section 2701 was enacted as part of the Electronic Communications Privacy Act of 1986 ("SCA"), Pub. L. No. 99-508, 100 Stat. 1848 (1986), and, consequently, codified the computer technology of 1986. The SCA distinguishes between providers of electronic communication service ("ECS") and providers of remote computing service ("RCS") to determine the level of protection afforded to communications stored therein. Although the ECS/RCS has been rendered practically obsolete by advances in technology, the distinction continues to matter because section 2701, the criminal provision of the SCA, has a narrow scope and *only* applies to providers of ECS and *only* to un-opened email. 18 U.S.C. § 2701(a)(1). See Kerr, *User's Guide* at 1239 ("The legislative history does not explain why [2701 only applies to ECS], but the approach is consistent with the SCA's greater protection for files held by providers of ECS than files held by providers of RCS.") Id. at 1240 ("[Section] 2701 comes with a significant cost: its vague language has needlessly confused the courts . . . . [S]everal of the major judicial interpretations of the SCA arise from the § 2701 cases

and misinterpret the SCA almost beyond recognition."); H.R. Rep. No. 99-647, at 64-65 (noting that opened e-mail stored on a server are protected under provisions relating to RCS.

Here, the Indictment fails to allege that Mr. Kernell read un-opened emails such as would subject him to liability under the limited scope of section 2701. Although an indictment will usually be sufficient if it states the offense using the words of the statute itself, Hamling v. United States, 418 U.S. 87, 117 (1974), the Supreme Court has cautioned, however: "Undoubtedly the language of the statute may be used in the general description of the offense, but it must be accompanied with such a statement of the *facts and circumstances* as will inform the accused of the specific offense, coming under the general description with which he is charged." Hamling, 418 U.S. at 117-18 (citation omitted) (emphasis added). Conclusory statements of fact in the indictment are insufficient. See United States v. Landham, 251 F.3d 1072, 1081 (6th Cir. 2001) (citing and applying Hamling standard, finding indictment insufficient and reversing convictions).

The indictment must be sufficiently detailed to "inform the court of the *facts* alleged, so that it may decide whether they are sufficient in law to support a conviction, if one should be had. For this, facts are to be stated, not conclusions of law alone." United States v. Cruikshank, 92 U.S. at 558. "An indictment that requires speculation on a fundamental part of the charge is insufficient." United States v. Bobo, 344 F.3d 1076, 1084 (11th Cir. 2003) (dismissing health care fraud indictment). Mr. Kernell is forced to speculate about a fundamental part of this Indictment; it must be dismissed.

V. THE INDICTMENT AND THE STATUTE UPON WHICH IT IS BASED ARE UNCONSTITUTIONALLY VAGUE.

Even if the Indictment is allowed to stand as a statutory matter, it must be dismissed because there is confusion surrounding the meaning and scope of the provisions alleged to have

been violated. A criminal statute is void for vagueness if it encourages arbitrary and discriminatory enforcement of the law. Papachristou v. City of Jacksonville, 405 U.S. 156, 162 (1972) ("Living under a rule of law entails various suppositions, one of which is that '(all persons) are entitled to be informed as to what the State commands or forbids.'") (quoting Lanzetta v. New Jersey, 306 U.S. 451, 453 (1939)).

> Although it is not likely that a criminal will carefully consider the text of the law before he murders or steals, it is reasonable that a fair warning should be given to the world in language that the common world will understand, of what the law intends to do if a certain line is passed. To make the warning fair, so far as possible the line should be clear.

McBoyle v. United States, 283 U.S. 25, 27 (1931).

The degree of vagueness that is constitutionally permissible, as well as the relative importance of fair enforcement, depends at least in part on the nature of the statute at issue. For example, economic regulations are subject to a less strict vagueness test, and courts have permitted tolerance of enactments with civil rather than criminal penalties, "because the consequences of imprecision are qualitatively less severe." Hoffman Estates v. Flipside, 455 U.S. at 499-500. Where a statute imposes criminal penalties, the standard of certainty required is higher. Kolender v. Lawson, 461 U.S. at 358-59 n.8; Winters v. New York, 333 U.S. 507, 515 (1948) (noting that a scienter requirement may mitigate a law's vagueness with respect to the adequacy of notice). Vagueness analysis is instructive when a statute uses technical terminology, especially when, as here, the statute uses antiquated technical terminology.

In this case, the Indictment suffers from two types of vagueness: vagueness on its face and vagueness as applied. Because Mr. Kernell is facing a criminal penalty, the standard of certainty must be higher, and because the Indictment and the statute upon which it is based do

not provide that certainty, Mr. Kernell was not given fair warning that his actions violated the law, and the Indictment must be dismissed as unconstitutionally vague.

a. *The statutes Mr. Kernell is alleged to have violated are facially vague.*

The statutes Mr. Kernell is charged with violating are facially vague. Both section 1030 and section 2701 contain aggravated penalty provisions to punish those offenders who commit the respective offenses "in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or any State." 18 U.S.C. § 1030(c)(2)(B)(ii); 18 U.S.C. § 2701(b)(1). The number and of type of crimes and torts which may be used to enhance the penalty for violating these statutes is conceptually unlimited, and growing. Cf. Paul Rosenzweig, *The Overcriminalization of Social and Economic Conduct*, The Heritage Foundation Legal Memorandum, Apr. 17, 2002, at 2 available at http://www.heritage.org/Research/LegalIssues/upload/40268_1.pdf ("Estimates of the current size of the body of federal criminal law vary. It has been reported that the Congressional Research Service cannot even count the current number of federal crimes. . . . More than 40 percent of these laws have been enacted in just the past 30 years . . . . And these laws are scattered in over 50 titles of the United States Code, encompassing roughly 27,000 pages."). Because the number of "crimes or tortious acts" which can be used to transform a misdemeanor into a felony is only limited by a prosecutor's imagination, the statute does not place any checks or balances on prosecutorial discretion. The result is that one cannot know in advance how or whether he or she will be punished.[5] See City of Chicago v. Morales, 527 U.S. 41, 56 (1999) (noting that under Supreme Court's vagueness jurisprudence, law is void if it "fail[s] to provide the kind of notice that will enable ordinary people to understand what conduct it prohibits").

[5] A person in Mr. Kernell's postion could not have foreseen that accessing someone's Yahoo! e-mail would result in a felony charge based on the use of section 2701. Since 2001, only ten individuals have pleaded guilty to violating section 2701, an average of less than two *per year*. See Federal Justice Statistics Resource Center, online at http://fjsrc.urban.org/analysis/t_sec/stat.cfm (last visited Oct. 22, 2008).

Congress has retained a misdemeanor section1030 violation, even while other parts of the statute have been repeatedly amended. See Majid Yar, *Cybercrime and Society* 40 (2006) (discussing history of the Computer Fraud and Abuse Act and noting that the Act has been amended in "response to technological innovations and new forms of computer crime . . . on numerous occasions (1986, 1989, 1990, 1994, and 1996) . . . [and that] significant amendments to the CFAA were introduced by the USA Patriot Act of 2001 . . . [which] included the increase of maximum penalties"). If the Government is allowed to enhance Mr. Kernell's charge of unauthorized access from a misdemeanor to a felony by alleging that he accessed the computer without authorization in furtherance of unauthorized access, the misdemeanor provision will have been effectively written out of the statute.

Even if this Court finds that "any criminal or tortious act" is not facially unconstitutionally vague, this Court must construe the phrase narrowly such that only those crimes or torts which necessarily do *not* occur whenever there is unauthorized access should be allowed to be used to enhance the predicate alleged violation.[6] Because, in this case, the Government has alleged no fact that would distinguish Mr. Kernell's alleged conduct from a misdemeanor or make it morally or functionally any worse than the basic misdemeanor, the charge is unconstitutionally vague.

The statute contains another, related defect: 1030(a)(2)(C) makes it a crime to obtain "information," a term undefined in the Computer Fraud and Abuse Act, and which is unhelpfully defined by Webster's as, "the communication or reception of knowledge or intelligence." Webster's Ninth New Collegiate Dictionary 620 (1983). In other words, section 1030 makes one liable for obtaining anything and everything. The unlimited scope of information which makes

[6] Compare the approach here to other offenses that contain enhancements when committed during or in furtherance of other crimes. Felony murder, for example requires the commission of a specifically enumerated offense. Tenn. Code Ann. § 39-13-202(a)(2).

one liable is underscored by courts' interpretation of "obtain." See S. Rep. 99-432, at 6 (1986) reprinted in 1986 U.S.C.C.A.N. 2479, 2484 (suggesting that one "obtains" a communication simply by viewing it on one's computer screen).

b. The statutes Mr. Kernell is alleged to have violated are vague as applied.

The Indictment cites[7] section 2701 of the Stored Communications Act ("SCA") as an aggravating factor to enhance 1030(a)(2). Section 2701 is violated when one

> intentionally accesses without authorization a facility . . . and thereby obtains . . . [an] electronic communication while it is in electronic storage in such a system.

18 U.S.C. § 2701(a). As applied to enhance the alleged violation of section 1030(a)(2) from a misdemeanor to a felony, section 2701 is unconstitutionally vague because there are divergent interpretations of the meaning of "electronic storage," one of 2701's elements.[8]

Although "electronic storage" is defined within the Act, any clarity its meaning once had has since been obscured by two decades of technological development. See 18 U.S.C. § 2510(17) (defining "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof," including backup copies of files in such temporary storage); see also *A Thinly Veiled Request for Congressional Action on E-mail Privacy:* United States v. Councilman, 19 Harv. J.L. & Tech. 211, 216 (2005) ("The lack of clarity [in the ECPA] results primarily from the fact that the language used –

[7] The Indictment does not, however, include the elements of 2701. Indictment ¶ 10.

[8] See also FTC v. Netscape Comm. Corp., 196 F.R.D. 559, 560 (N.D. Cal. 2000) (holding that a provider of email accounts over the Internet is a provider of ECS); S. Rep. 99-541, at 8 (1986), reprinted in 1986 U.S.C.C.A.N. 3555 (describing the functioning of an email system in terms that can encompass a web-based service: "[i]n its most common form, messages are typed into a computer terminal, and then transmitted over telephone lines to a recipient computer operated by an electronic mail company."). But see Crowley v. CyberSource Corp., 166 F. Supp. 2d 1263 (N.D. Cal. 2001) (holding that Amazon.com did not meet the SCA drafters' definition of ECs because Amazon.com "must itself purchase Internet access from an electronic communication service provider . . . it does not independently provide such services"); In re Northwest Airlines Privacy Litigation, No. Civ.04-126 (PAM/JSM), 2004 WL 1278459 (D. Minn. June 6, 2004) (holding that Northwest was not an ECS because Northwest was not an ISP and had to "purchase [] its electronic communications). The ECS/RCS distinction matters because section 2701, the criminal provision of the SCA, has a narrow scope and *only* applies to providers of ECS. 18 U.S.C. § 2701(a)(1).

"communication" versus "storage," "intercept" versus "access" – does not correspond to the technical realities of e-mail: e-mail messages can shift from transit to storage and back in nanoseconds."); id. at 221 (quoting from United States v. Councilman, 373 F.3d 197, 204 (1st Cir. 2004), in which a panel of the First Circuit concluded that "[a]lthough the ECPA no longer reflected the realities of e-mail communication, 'it is not the province of [the] court to graft meaning onto the statute where Congress has spoken plainly.'").

Section 2701 was enacted as part of the Electronic Communications Privacy Act of 1986 ("SCA"), Pub. L. No. 99-508, 100 Stat. 1848 (1986), to create a statutory expectation of privacy in electronic files, because electronic files are revealed to third-parties multiple times during each transmission,[9] and the Fourth Amendment does not protect information revealed to third-parties. See United States v. Miller, 425 U.S. 435, 443 (1976) ("[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party. . . ."); see also United States v. Bach, 310 F.3d 1063, 1068 (8th Cir. 2002) ("While it is clear to this court that Congress intended to create a statutory expectation of privacy in e-mail files, it is less clear that an analogous expectation of privacy derives from the Constitution.").

In spite – or perhaps because – of the fact that the statute was enacted over twenty years ago, the SCA "remains poorly understood." Kerr, *User's Guide* at 1208 ("The statute is dense and confusing, and few cases exist explaining how the statute works."). For example, though enacted to fill the Fourth Amendment gap in privacy protection for electronic files, the SCA

[9] "[M]ultiple transitory copies of an e-mail's content are created as it moves across the network from sender to recipient. The existence of static copies of the e-mail communication's content, which can be accessed after the fact from entities not party to the communication, is distinct from traditional voice communications over a wire which, because of its ephemeral nature, can only be accessed by eavesdropping in real-time through the cooperation of a party to the communication." Deidre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective of the Electronic Communications Privacy Act*, 72 Geo. Wash. L. Rev. 1557, 1558 (2004).

provided different levels of protection for different types of information, and it made such distinctions based on the types of technology prevalent in the 1980s:

> The SCA adopts these two distinctions, freezing into the law the understandings of computer network use as of 1986. The text regulates two types of providers: providers of electronic communication service ("ECS") and providers of remote computing service ("RCS"). . . .
>
> What does this mean in practice? Some cases are easy. For example, when an e-mail sits unopened on an ISP's server, the ISP is acting as a provider of ECS with respect to the email. . . . [However] the proper treatment of opened email is currently unclear. **The traditional understanding has been that a copy of opened e-mail sitting on a server is protected by the RCS rules, not the ECS rules.** The thinking is that when an e-mail customer leaves a copy of an already-accessed e-mail stored on a server, that copy is no longer "incident to transmission" nor a backup copy of a file that is incident to transmission: rather, it is just in remote storage like any other file held by an RCS.

Kerr, *User's Guide* at 1213-16 (emphasis added). The "traditional understanding" that opened email is not protected under section 2701 has been called into question by a Ninth Circuit holding that all e-mails held by a server are protected until "the underlying message has expired in the normal course," regardless of whether the e-mail has been accessed. Theofel v. Farey-Jones, 359 F.3d 1066, 1077 (9th Cir. 2004) ("[W]e think that prior access is irrelevant to whether the messages at issue are in electronic storage."). However, the Department of Justice, as recently as 2007, rejected the Theofel interpretation:

> The term "electronic storage" has a narrow, statutorily defined meaning. It does *not* simply mean storage of information by electronic means. . . . If the communication has been received by a recipient's service provider but has not yet been accessed by the recipient, it is in "electronic storage" . . . .
>
> If Theofel's broad interpretation of "electronic storage" were correct, prosecutions under section 2701 would be substantially less difficult, as it can be hard to prove that communications fall within the traditional narrow interpretation of "electronic storage." However CCIPS continues to question whether Theofel was correctly decided, since little reasons exists for treating old email differently than other material a user may choose to store on a network.

Dep't of Justice, *Computer Crime* at 80-81. See also Bansal v. Russ, 513 F. Supp. 2d 264, 276 (E.D. Pa. 2007) (holding that "to the extent Plaintiff purports to assert claims for violation of the Stored Communications Act based on the government's obtaining of 'opened' e-mails, the claims must be dismissed because such conduct, even if proved, does not violate the Act"); Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623, 635-38 (E.D. Pa. 2001) (concluding that e-mails taken from post-transmission storage are not in "electronic storage").

When the Theofel decision is examined, it becomes clear that the traditional understanding embraced by the Department of Justice is the interpretation this Court should use to dismiss the felony enhancement. In Theofel, the court was faced with an overly broad subpoena for e-mail issued as part of the discovery process in a *civil* commercial dispute. Id. at 1071-72. According to one scholar, the problem with the Ninth Circuit's interpretation stems from this simple fact: the plaintiffs sued under the wrong statute.

> The plaintiffs . . . should have sued under §2703: defendants had violated § 2703 by using improper legal process to compel the disclosure of e-mail from and ECS/RCS in violation of § 2703(a) and (b). The plaintiffs instead sued under § 2701, contending that the defendants had caused the ISP employees to commit an unauthorized access of their own server when the retrieved the files from the server and posted them on the website. This is a strange claim, and agreeing with it required creating new, expansive, and (in some cases) extraordinary interpretations of several key concepts in computer crime law: the meaning of authorization, the meaning of access, the scope of ECS protections, and the scope of provider rights. But eager to find a violation and apparently unaware of how plainly these facts fit into § 2703, Judge Kozinski charged onwards and crafted a dubious theory under which the plaintiffs could win under §2701.

Id. at 1240.

The Indictment therefore suffers from vagueness because either (1) the Department of Justice is taking a contrary position to the traditional understanding of 2701, in which case there is a non-reconcilable split between interpretations such that a reasonable person is not put on notice, or (2) if the Government is following its manual and has charged according to the

traditional definition, then the Indictment fails to state the factual predicate that Mr. Kernell read unopened e-mails.

Finally, the statutes upon which this Indictment is based are vague as applied because they are prosecuted infrequently and unpredictably. Papachristou v. City of Jacksonville, 405 U.S. 156, 162 (1972) (holding that a criminal statute is void for vagueness if it encourages arbitrary and discriminatory enforcement of the law). Contrary to the statement made by a representative of the FBI in the Department of Justice's press release about Mr. Kernell, there is a growing disparity between the number of computer crimes committed and the number of computer crimes charged. Compare *David C. Kernell Indicted for Alleged Hack of Governor Sarah Palin's E-mail Account* available at http://www.usdoj.gov/usao/tne (last visited Oct. 21, 2008) ("Cyber crime is the FBI's top criminal investigatory priority.") with Orin S. Kerr, *Enforcing Law Online*, 74 U. Chi. L. Rev. 745, 758 (2007) ("Although every computer connected to the Internet is subject to frequent attacks by outsiders, the federal government only brings criminal charges for computer hacking against about one hundred defendants per year.") (citing the Federal Justice Statistics Resource Center's dataset which indicates that in 2004, ninety-four defendant were charged under 18 U.S.C. § 1030). See also Deidre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 Geo. Wash. L. Rev. 1557, 1575 (2004) ("Approximately 102 million U.S. individuals use e-mail, with about 60 million using it on any given day."); Majid Yar, *Cybercrime and Society* 40, 15 (2006) (noting that "[g]aining a realistic measure of the scope and scale of cybercriminal activities presents considerable challenges," but estimating that as of 2001, there were 66,000 computer viruses in existence and that a credit card fraud occurs every 20 seconds).

VI. CONCLUSION

The Government has improperly joined two misdemeanor provisions in an attempt to create a felony. The Indictment must be dismissed because this prosecution is based on unconstitutionally vague statutes, particularly as these two misdemeanors are aggregated into a felony.

Respectfully submitted this 27th day of October, 2008.

RITCHIE, DILLARD & DAVIES, P.C.

/s/ WADE V. DAVIES
WADE V. DAVIES [BPR #016052]
ANNE E. PASSINO
606 W. Main Street, Suite 300
P. O. Box 1126
Knoxville, TN 37901-1126
(865) 637-0661

Counsel for David C. Kernell

CERTIFICATE OF SERVICE

The undersigned hereby certifies that a true and exact copy of the foregoing has been filed electronically this 27th day of October, 2008. Notice of this filing will be sent by operation of the Court's electronic filing system to all parties indicated on the electronic filing receipt. Parties may access this filing through the Court's electronic filing system.

/s/ Wade V. Davies
WADE V. DAVIES